SIEM

What is SIEM?

Security

Incident

&

Event

Management

What does it mean to you?

SECURITY Incident & Event Management

- 44 U.S.C. § 3542(b)(1)
  - (1) The term “information security” means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—
    - (A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;
    - (B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
    - (C) availability, which means ensuring timely and reliable access to and use of information.
- Weight of each (A, B, C) unique to an organization
- Value of each is also unique
- Security disposition or posture is informed by the **risk** profile of the organization to shape **policy** in order to define operations through **procedures** and **guidelines**.

Security INCIDENT & Event Management

- An occurrence of significance
- Generally considered to be an event that impacts an established **policy** (clear) or expectation (unclear)
- Actionable

Security Incident & EVENT Management

- An occurrence
- Quantifiable within an operational context
- Informational

Security Incident & Event MANAGEMENT

- Act of handling or controlling
- Governed by an established set of **procedures** and **guidelines** for operational conduct

SIEM Challenges

- Staffing
- Proactive management
- Incident response teams
- Incident response procedures
- Alignment with business requirements

What do you really need to do?

The Need for Operational Insight

- Security Information Management
  - Investigate security and network operational events
  - Visualize current state
  - Operational metrics
  - Typically reactive
  - Aligns with small to medium businesses more readily

How do we get there?

- Raw information flow to a central point
- Cohesion of raw data into events of meaning
- Correlation of events into incidents
- Evaluation of incidents by profile to determine criticality
- Validation of incidents to targets to modify criticality
- Presentation layer for centralized information
- Measurement of incident
- Summarization of incident measurements into metrics
- Tracking of metrics over time
- Comparison of metrics tracking to baselines (internal and external)

Systems and Methodologies

- Logging
  - Distributed/localized
  - Centralized logging of similar log types
  - Centralized logging of dissimilar log types
- Collection of asynchronous data
- Evaluation against real-time signatures
  - Detection systems
  - Prevention systems
- Analysis and event recognition
- Event correlation
- Event detection and alerting
- Compliance auditing and validation

Additional Terminology

- Log message, message, or log record
  - Individual entry corresponding to a single action or state
- Log or logfile
  - Record or file containing log messages
- IDS, IPS, IDP
  - Intrusion Detection/Prevention System
  - Intrusion Detection and Prevention

Raw Information

- Source: Logs
- Logs = Accountability
- *Orange Book:*

> *Requirement 4: ACCOUNTABILITY - Audit information must be selectively kept and protected so that actions affecting security can be traced to the responsible party. A trusted system must be able to record the occurrences of security-relevant events in an audit log*

Logging Challenges

- Too much data
- Not enough data
- Poor information delivery
- False positives
- Hard-to-get data
- Redundant and inconsistent data
- Heterogeneous IT environments

Log Management

- Logging Configuration
  - Log collection
  - Log standards
  - Log storage & integrity
  - Log analysis
- Information Presentation
- Automation
- Compliance requirements

Logging Targets

The following targets are listed from most obvious to least obvious with increasing challenge to gather such logs

- Network devices
  - Switches, routers, etc.
- Security devices
  - Perimeter, proxy, monitoring, filtering, etc.
- Servers
  - Applications, messaging, directory services, file services
- Endpoint
  - A/V, malware, personal FW, applications, etc.
- Physical Security
  - Access, resource utilization

Asynchronous Data Sources

- Organization is more than a set of technologies
- HR initiatives
- Security programs
- Project management
- Supply & logistics

Cohesion

- Incident Detection
  - Event Signatures
- Relevance
- Context
- Correlation
- Watch Lists

Resilient Detection and Analysis

- Requires centralized logging of dissimilar systems with event correlation
- Example
  - IDP system detects exploit via signature
  - Firewall reports targeted system initiating outbound ftp
  - Targeted system logs change to registry
  - Targeted system initiates “puts” to internal file sharing systems
  - IDP system detects outbound exploits via same signature from target
  - High port UDP connection outbound to known botnet command and control
  - Excessive traffic initiated outbound to e-commerce site from target

Data to Incidents to Metrics

What are Security Metrics and why are we talking about them?

- Measurement – Single point in time view
- Metric – multiple measures over time with a baseline and / or target
- Security vs. Risk Management
  - Security is absolute – zero tolerance
  - Risk management is relative – the degree of tolerance

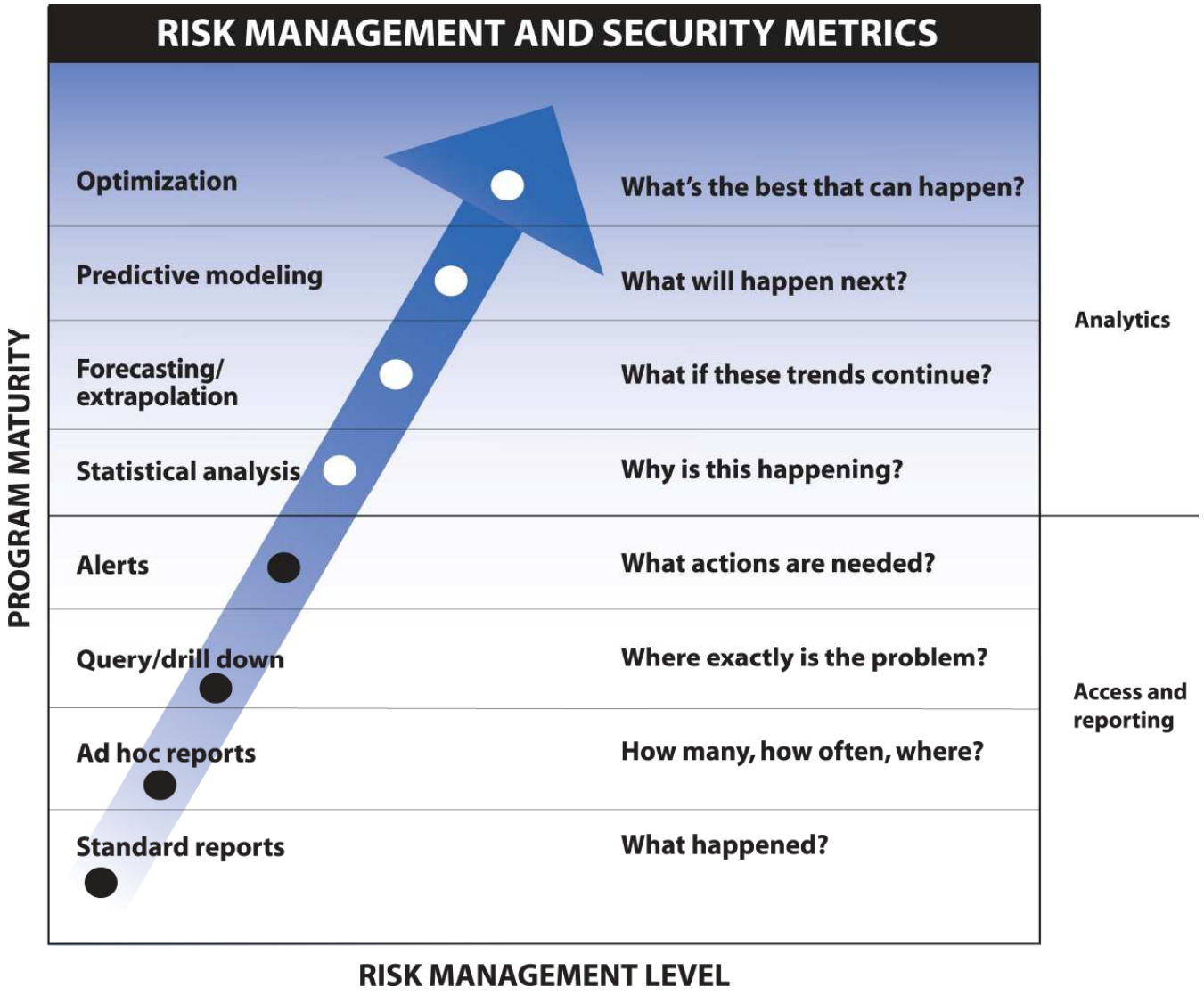
High level goals...

- Obtain alignment throughout the organization.
- Identify objectives so we know where we are going.
- Prioritizing initiatives that guide the metrics program.
- Gather business and technical requirements.
- Promote organization wide adoption and acceptance

Analytics Stages Model

Level	Visibility	Questions Asked	Objective	Metrics Program Value
0 Non-Existent	Obscured or indirect	Are the IT resources available?	Obtain data for troubleshooting IT related problems. Policy (or process) is not documented, and previously the organization was unaware of the business risk associated with this risk management.	None
1 Ad-Hoc	Component or situational data	Can we research what happened in a security and risk management context?	Obtain information for select people in the or organization that recognize that risk management has value.	Support Risk Management program development
2 Defined & Repeatable	Scheduled Meaningful Reports	How do our security trends compare with our risk management objectives?	Implement a security metrics program that is integrated with a risk management program and has visibility throughout the organization.	Security metrics are integral in the risk management process
3 Actionable Process	Information and Alerts are timely and integrated with operational processes	What information can we use to operationally improve risk management?	Implement a formal risk management program with operational integration throughout the organization.	Security metrics provide input for operationally integrated risk mitigation.
4 Planned & Managed	Comprehensive information and reports linked to objectives and plans	Are we planning effectively to meet our risk management objectives? Are we managing t to meet our plans?	Develop a thorough understanding of risk management at all levels of the organization. Implement a risk management and security metrics program to effectively plan and implement risk mitigation initiatives.	Security metrics provide a reliable feedback loop and are used for planning and management purposes.
5 Optimized	Dynamic security metrics that are clearly aligned with a risk management strategy. Predictive and comparable results with measurable improvement.	How accurate are our risk management targets? How good can we get?	Fully integrate risk management and security metrics into the culture of our organization. Use metrics to drive continuous improvement.	Security metrics are used to optimize economic value for the firm now and in the future.

Risk Management and Security Metrics



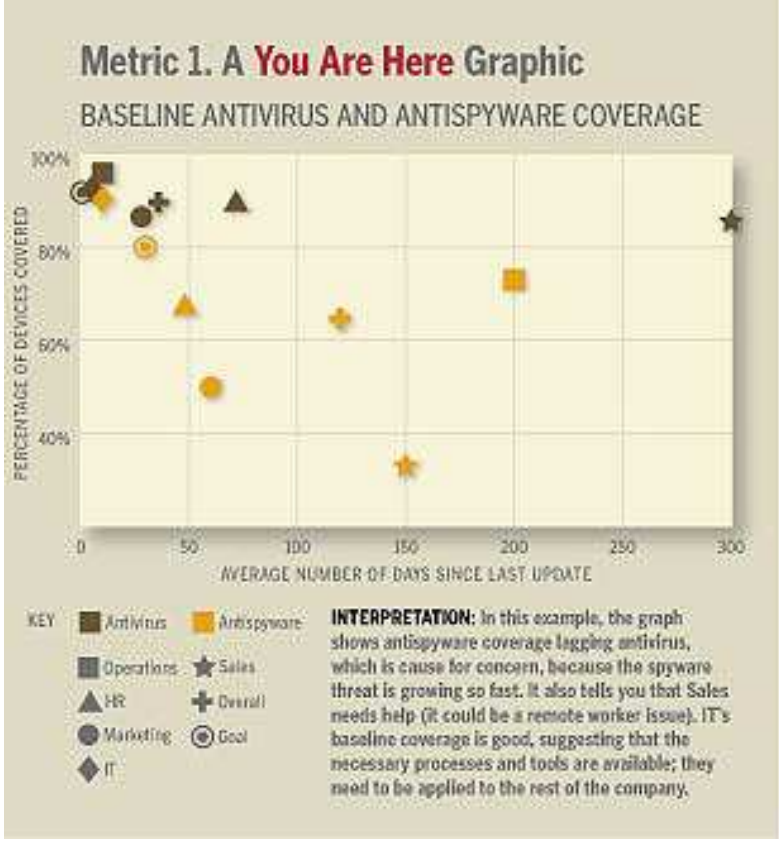
Implementing Metrics in Security Operations

Metric 1 – Endpoint Defenses

- Percentage of systems with up-to-date endpoint defenses (antivirus, anti-spam, firewall, HIDS agent)
- Vetting method - ability to execute a harmless exploit, like embedding "sniper.exe" in Adobe PDF.

Metric 2 – Patch Latency

- Number of days between patch release and deployment to target saturation rate.
- Vetting method - vulnerability detection via vulnerability management program (scan, detect, report, mitigate and validate)



Source:http://www.csoonline.com/article/220462/A_Few_Good_Information_Security_Metrics

Metric 3 - Password Compliance

- Percentage of active accounts with password that meets password policy (length, strength, expiration).
- Vetting method - average length of time to crack a typical password.

Metric 4 - Platform Compliance

- Percentage of systems that exceed target benchmark scores.
- Vetting method - CIS Benchmark* results compared against vulnerability management policy compliance checks.

Source: http://www.csoonline.com/article/220462/A_Few_Good_Information_Security_Metrics

Considerations

- Clearly identify expectations for the system
- Will you monitor the system?
  - Alert & Response
  - Proactive visibility
  - Staffing
- Will you analyze the system?
  - Research and investigate for patterns of activity
  - Staffing
- Reporting
  - Interval
  - Stakeholders/consumers
  - Dashboard

Discussion Questions

- How does IT Governance and regulatory compliance affect event logging?
- Is your security event logging implementation aligned with your security policies?
- What security events and logs are relevant to analyze and retain?
- Who is responsible for gathering maintaining and monitoring your log information?
- What is the optimal retention period and reporting frequency?

Q & A

- Q & A
- Thank you!